Draft Meeting Minutes
Maryland Cybersecurity Council
Subcommittee on Critical Infrastructure
Wednesday, June 1, 2022
1:00 pm – 2:00 pm
Virtual Public Meeting

Member Attendance (6/10)
Subcommittee members attending: Markus Rauschecker (chair), John Abeles, Dr. David Anyiwo, Jessica Curtis (for David Engel), Fred Hoover, and Clay House.

Guest presenters: Michael Block (Chair, Cybersecurity Standards Committee, ENSB), Josh Jack (Mission Critical Partners) and John Borkowski (Chief Engineer, Public Service Commission)

Staff: Howard Barr (Assistant Attorney General and Principal Counsel, DoIT) and Dr. Greg von Lehmen (University of Maryland Global Campus, Staff to the Maryland Cybersecurity Council)

Meeting Summary

1. The chair welcomed the members and invited speakers and reviewed the agenda.
2. The minutes for the 04 October 2021 meeting of the subcommittee were unanimously approved after motions duly made.
3. The subcommittee then turned to the other business on the agenda:

Updates

- *2022 session and critical infrastructure*. The chair provided an overview of bills in the last legislative session that concerned State and local government cybersecurity and the electric grid. The following were signed into law by the Governor:

    - SB 812 (State Government – Cybersecurity – Coordination and Governance)
    - SB 754 (Local Government Cybersecurity – Coordination and Operations (Local Cybersecurity Support Act of 2022)
    - HB 1205 (State Government – Information Technology and Technology and Cybersecurity–Related Infrastructure (Modernize Maryland Act of 2022)

    The chair noted that the bill (SB 810/HB 1339) which would have implemented some of the recommendations of the special report completed for the Council on the grid was withdrawn during session.

    Next Gen 911. Mr. Bock and Mr. Jack provided three principal updates:

- The cybersecurity standards subcommittee was compiling guidance on cybersecurity best practices for the new system. As guidance, the best practices will not be mandatory.
- A training session and tabletop exercise is being planned for the fall that will include the public service access points (PSAPs) and vendors. The training session will include multiple presentations by the State and the Critical Infrastructure Protection Agency (CISA), among others.
- Another round of cybersecurity preparedness assessment and remediation planning is underway with the PSAPs.

New business.

Maryland Public Service Commission. Mr. Borkowski's presentation provided background on the cybersecurity efforts of the Public Service Commission (PSC) to date, recapped the utility requirements, and concluded with a description of proposed regulations. Key points included:

- The PSC's approach to cybersecurity has evolved. Commission Order 85680 established a cybersecurity reporting process for the smart grid initiatives of BGE, PEPCO, and Delmarva. In 2016, these companies, joined by Washington Gas and Potomac Edison, provided cybersecurity briefings in 2016. In 2017, the Commission established a cybersecurity working group whose recommendations became the basis of Commission Order 89015. Among other things, this order required periodic cybersecurity briefings under certain protocols on a schedule for utilities of a certain size and also mandated the reporting of cybersecurity incidents.
- The cybersecurity working group has proposed additional regulations that have been informed by the briefings that have occurred to date. These have been announced in the Maryland Register (RM 76) and will be voted on by the Commission on June 29. Among other things, the proposed regulations would require utilities to follow good cybersecurity practice and to have cybersecurity plans that address cybersecurity-related governance, risk management, procurement practices, personnel hiring, training policies, situational awareness, response, recovery, and transparent reporting of cybersecurity incidents to State and federal entities. (See presentation Appendix [Proposed Regulations, Title 20, Subtitle 06]).

Mr. House asked Mr. Borkowski whether the PSC might consider safe harbor for early notification of a breach. This would encourage utilities to report breaches before they are sure that a breach in fact has occurred to provide the PSC was situational awareness more quickly. Mr. Borkowski answered that the PSC has not discussed such an approach.

Mr. Rauschecker whether reported incidents are shared anywhere to create greater situational awareness. Mr. Borkowski answered the Commission is not an information sharing entity.

Dr. von Lehmen asked if the working group or the Commission might consider specifying standards or a menu of standards for utilities. Mr. Borkowski answered that this is not on the agenda for the immediate future. But the steps the Commission is taking are not the end and will continue to evolve. The matter of standards is complicated. There are many applicable standards, and the working group is looking at some of them.

Subcommittee initiatives for the future. As an initial discussion, five ideas were surfaced by the members:

- Creating a Critical Infrastructure Fellow program as a resource for the PSC
- Locating innovative security tools, whether used in the US or abroad, that might be cost effective for utilities to us.
- Identifying innovative commercial security tools that could be brought into State government.
- Creating a discussion platform where new approaches to security could be discussed.
- Study the resiliency of the utility sector with the subcommittee making periodic reports.

Other business & Adjournment

There being no further business, the subcommittee adjourned at 2:38 pm.